Appendix A High Level Requirements Traceability Matrix

No	Requirement The System Shall…	Area	Sub-Area	Use Case
1	Allow an administrator to enroll new users for the mDL program	Core Functions	Administrative Functions	Enroll in the mDL Program
2	Allow an administrator to associate an existing traditional driver's license with a mDL	Core Functions	Administrative Functions	Enroll in the mDL Program
3	Allow an administrator to view existing mDL enrollments	Core Functions	Administrative Functions	Enroll in the mDL Program
4	Provide the ability to determine if a prospective user is eligible for enrollment into the mDL program	Core Functions	Administrative Functions	Enroll in the mDL Program
5	Allow an administrator to cancel the mDL enrollment process	Core Functions	Administrative Functions	Enroll in the mDL Program
6	Capture requests for enrollment into the mDL program	Core Functions	User Functions	Enroll in the mDL Program
7	Present disclaimers, terms and conditions for new enrollments in to the mDL program	Core Functions	User Functions	Enroll in the mDL Program
8	Ensure that disclaimers, terms and conditions for new enrollments in to the mDL program have been accepted before enrolling the user	Core Functions	User Functions	Enroll in the mDL Program
9	Create a record that the disclaimers, terms and conditions for new enrollments in to the mDL program have been accepted	Core Functions	User Functions	Enroll in the mDL Program
10	Allow new users enroll in the mDL program	Core Functions	User Functions	Enroll in the mDL Program
11	Provide the user with a single use secure credential to be used for initially authenticating the user's identity through their mobile device	Core Functions	User Functions	Enroll in the mDL Program
12	Deliver instructions for acquiring and configuring the mDL application to the user	Core Functions	User Functions	Enroll in the mDL Program
13	Capture requests for enrollment into the mDL program	Core Functions	User Functions	Enroll in the mDL Program
14	Allow the user to cancel the mDL enrollment process	Core Functions	User Functions	Enroll in the mDL Program
15	Notify a user that their mDL has been issued	Core Functions	User Functions	Procure a mDL
16	Provide a means for the user to install or enable mDL application on their mobile device	Core Functions	User Functions	Procure a mDL
17	Provide a means for the user to access the mDL application on their mobile device	Core Functions	User Functions	Procure a mDL
18	Authenticate a user's secure single use credential	Core Functions	User Functions	Procure a mDL
19	Allow initial login to the mDL application using a single use credential	Core Functions	User Functions	Procure a mDL
20	Ensure that a user creates new credentials after their first login to the mDL	Core Functions	User Functions	Procure a mDL
21	Enable display of mDL only after a user has logged in using their credentials	Core Functions	User Functions	Procure a mDL
22	Enable authentication of mDL only after a user has logged in using their credentials	Core Functions	User Functions	Procure a mDL
23	Associate privileges with a user mDL	Core Functions	Administrative Functions	Update privileges associated with a mDL
24	Allow administrators to add associated privileges to a user mDL	Core Functions	Administrative Functions	Update privileges associated with a mDL
25	Allow administrators to remove associated privileges from a user mDL	Core Functions	Administrative Functions	Update privileges associated with a mDL
26	Allow administrators to suspend privileges associated with a user mDL	Core Functions	Administrative Functions	Update privileges associated with a mDL
27	Allow administrators to reinstate privileges associated with a user mDL	Core Functions	Administrative Functions	Update privileges associated with a mDL

28	Notify a user that the privileges associated with their mDL have been updated	Core Functions	User Functions	Update privileges associated with a mDL
29	Update the privileges displayed on a mDL to reflect updates made by administrators	Core Functions	User Functions	Update privileges associated with a mDL
30	Update the privileges that can be presented with a mDL to reflect updates made by administrators	Core Functions	User Functions	Update privileges associated with a mDL
31	Prevent authentication of the mDL unless the user permits it	Core Functions	User Functions	Authenticate mDL
32	Prevent access to the mDL unless the user authenticates using secure credentials	Core Functions	Technical	Authenticate mDL
33	Allow an authenticator to validate an mDL	Core Functions	Authentication Functions	Authenticate mDL
34	Allow an authenticator to flag abuse of a mDL	Core Functions	Authentication Functions	Authenticate mDL
35	Notify the administrator of mDLs that have been flagged for abuse	Core Functions	Administrative Functions	Authenticate mDL
36	Notify a user that their mDL has been flagged for abuse	Core Functions	User Functions	Authenticate mDL
37	Allow an administrator to invalidate a mDL that has been flagged	Core Functions	Administrative Functions	Authenticate mDL
38	Allow an administrator to reinstate a mDL that has been flagged	Core Functions	Administrative Functions	Authenticate mDL
39	Periodically synch and update the status of a mDL	Core Functions	Technical	Authenticate mDL
40	Present a timestamp on the mDL demonstrating the last update of the mDL	Core Functions	Technical	Authenticate mDL
41	Prevent access to view the privileges associated with the mDL unless the user permits it	Core Functions	User Functions	View privileges associated with a mDL
42	Display privileges associated with the users mDL	Core Functions	User Functions	View privileges associated with a mDL
43	Allow a user to select the subset of privileges to display	Core Functions	User Functions	View privileges associated with a mDL
44	Display personal information associated with the users mDL	Core Functions	User Functions	View mDL personal information
45	Allow a user to select the subset of personal information to display	Core Functions	User Functions	View mDL personal information
46	Prevent access to view the personal information associated with the mDL unless the user permits it	Core Functions	User Functions	View mDL personal information
47	Notify the user that a request to update their mDL information has been captured	Core Functions	Administrative Functions	Update mDL Personal Information
48	Allow the administrator to review requests for mDL information updates	Core Functions	Administrative Functions	Update mDL Personal Information
49	Allow the administrator to approve or deny requests for mDL information updates	Core Functions	Administrative Functions	Update mDL Personal Information
50	Display updated information on a users mDL	Core Functions	User Functions	Update mDL Personal Information
51	Provide administrators with the ability to dis-enroll existing users from the mDL program	Core Functions	Administrative Functions	Dis-enroll from the mDL Program
52	Provide users with the ability to dis-enroll from the mDL program	Core Functions	User Functions	Dis-enroll from the mDL Program
53	Ensure that users are authenticated when dis-enrolling from the mDL program	Core Functions	User Functions	Dis-enroll from the mDL Program
54	Ensure that users confirm their intent to dis-enroll from the mDL program	Core Functions	User Functions	Dis-enroll from the mDL Program
55	Provide a confirmation once a user has been dis-enrolled from the mDL program	Core Functions	User Functions	Dis-enroll from the mDL Program
56	Disable all mDL authentication and display functions on the user's devices once a user is dis-enrolled	Core Functions	User Functions	Dis-enroll from the mDL Program
57	Purge any mDL related data that is stored remotely once a user is dis-enrolled	Extended Functions	Technical	Dis-enroll from the mDL Program

58	Display a 2-d barcode that encodes the user's driver's license information	Extended Functions	Stakeholder Functions	Scan mDL barcode
59	The displayed 2-d barcode must be compliant with the existing standard used for physical driver's licenses	Extended Functions	Technical	Scan mDL barcode
60	Ensure that displayed 2-d barcode can be scanned with a barcode scanner (maximize brightness and contrast of the screen)	Extended Functions	Technical	Scan mDL barcode
61	Display the driver's license information of the user's mDL to an authenticator	Extended Functions	Authentication Functions	Authenticate mDL manually
62	Display the user's driver's license picture to an authenticator	Extended Functions	Authentication Functions	Authenticate mDL manually
63	Display security features (like a randomized token) that can be used by an authenticator to manually validate a mDL by calling into a hotline or dispatch	Extended Functions	Technical	Authenticate mDL manually
64	Provide the ability to authenticate with another digital device	Extended Functions	Technical	Authenticate mDL digitally, in a disconnected state
65	Provide the ability to communicate with another digital device	Extended Functions	Technical	Authenticate mDL digitally, in a disconnected state
66	Request permission from the user before initiating communication with another device	Extended Functions	Technical	Authenticate mDL digitally, in a disconnected state
67	Automatically revoke further access to communicate with a user's mDL after the interaction with the authenticator is complete	Extended Functions	Technical	Authenticate mDL digitally, in a disconnected state
68	Allow the mDL to remotely authenticate	Extended Functions	Technical	Authenticate mDL digitally, in a connected state
69	Provide secure remote attestation of user identity to digital authentication devices	Extended Functions	Technical	Authenticate mDL digitally, in a connected state
70	Allow the authenticator to remotely retrieve privileges associated with the mDL	Extended Functions	Technical	Authenticate mDL digitally, in a connected state
71	Allow the authenticator to remotely retrieve information associated with the mDL	Extended Functions	Technical	Authenticate mDL digitally, in a connected state
72	Allow a stakeholder or authenticator to digitally retrieve privileges associated with the mDL	Extended Functions	Technical	Electronically access mDL information
73	Allow a stakeholder or authenticator to digitally retrieve information associated with the mDL	Extended Functions	Technical	Electronically access mDL information
74	Request permission from the user to transmit privileges associated with the mDL to another device	Extended Functions	Technical	Electronically access mDL information
75	Request permission from the user to transmit information associated with the mDL to another device	Extended Functions	Technical	Electronically access mDL information
76	Automatically revoke further access to communicate with a user's mDL after transmission of information associated with the mDL to another device is complete	Extended Functions	Technical	Electronically access mDL information
77	Automatically revoke further access to communicate with a user's mDL after transmission of privileges associated with the mDL to another device is complete	Extended Functions	Technical	Electronically access mDL information
78	Notify a user that a request has been made to digitally transmit privileges associated with the user's mDL	Extended Functions	Use Functions	Electronically access mDL information
79	In order to facilitate interoperability across jurisdictions, the mDL, the mDL reader, and its related infrastructure will comply where possible with draft ISO18013 technical requirements. Any variances where the solution does not follow the draft ISO18013 technical requirements will be documented by the vendor and subject to Department approval.	Extended Functions	Technical	Electronically access mDL information
80	Notify a user that a request has been made to digitally transmit information associated with the user's mDL	Extended Functions	User Functions	Electronically access mDL information

81	Store a record certifying that a mDL has been digitally validated	Extended Functions	Technical	Record mDL validation
82	Return a key to the authenticator which corresponds to the record certifying that a mDL has been digitally validated	Extended Functions	Technical	Record mDL validation
83	Retrieve a record corresponding to an authentication key certifying that a mDL has been digitally validated	Extended Functions	Technical	Record mDL validation
84	Provide access to appropriate functions for mDL users, administrators, stakeholders and authenticators	Non-Functional	Accessibility	N/A
85	Provide a user interface that is navigable by and accessible to all users of supported mobile platforms (including those with disabilities)	Non-Functional	Accessibility	N/A
86	Integrate with the Iowa DoT's existing licensing and administrative systems, preserving their roles as systems of record	Non-Functional	Architecture/Integration	N/A
87	Be developed using an advanced approach to interoperability using web services and Service Oriented Architecture (SOA) allowing for all major administrative functions to be completed through Web Service APIs	Non-Functional	Architecture/Integration	N/A
88	Consist of a number of components and services that are compliant with industry standards for service-oriented architecture and Web Services (W3C, OASIS, etc.) to facilitate reuse, adaptability and interoperability	Non-Functional	Architecture/Integration	N/A
89	Ensure secured access to services based on defined security rules	Non-Functional	Architecture/Integration	N/A
90	Interface with Iowa DoT's systems of record through Web Service APIs and enable mDL program functions to be incorporated into the workflows of those systems	Non-Functional	Architecture/Integration	N/A
91	Provide audit-tracking reports for user access and usage logs including a detailed audit trail for a select set of system transactions, activities and actions, including date, time and author	Non-Functional	Audit	N/A
92	Have the ability to provide an audit trail for changes, additions and deletions to data, including operational and security data	Non-Functional	Audit	N/A
93	Be available for use 999% of the time (no more than 88 hours of downtime per year)	Non-Functional	Availability/Capacity	N/A
94	Operate 24 hours per day, 7 days per week, and 52 weeks per year	Non-Functional	Availability	N/A
95	Have the ability to support transparent failover using high-availability processor architectural options	Non-Functional	Availability	N/A
96	Be able to continue to operate despite failure or availability of individual technology components such as a server platform or network connection	Non-Functional	Availability	N/A
97	Be able to handle the initial launch storage and processing loads while growing to serve growth of the user base	Non-Functional	Capacity	N/A
98	Maintain compatibility with major supported mobile platforms (Android, iOS) and a defined range of OS versions	Non-Functional	Device Compatibility	N/A
99	Be compatible with leading devices (Apple iPhone, Samsung Galaxy S series, etc.) which support the hardware requirements of the mDL application	Non-Functional	Device Compatibility	N/A
100	Be compatible with a well defined range of mobile screen sizes, resolutions and form factors	Non-Functional	Device Compatibility	N/A
101	Be implemented such that the mDL application is not degraded as a result of minor OS version updates (e.g. use stable APIs, avoid deprecated features, avoid niche or dated 3rd party libraries etc.)	Non-Functional	Device Compatibility	N/A
102	Make use of platform standards and features developed by mobile platform makers (e.g. digital wallet APIs, biometric features, push notifications etc.)	Non-Functional	Device Compatibility	N/A
103	Be implemented to efficiently use the mobile battery and avoid unnecessary drain on the mobile devices processing resources	Non-Functional	Device Compatibility	N/A

104	Ensure the mDL application functions in a various states of connectivity (cellular data, wifi, disconnected etc.)	Non-Functional	Device Compatibility	N/A
105	Preserve data integrity, fail safe and trap bad data and faults	Non-Functional	Integrity	N/A
106	Be designed for ease of maintenance and readily allow future functional enhancements	Non-Functional	Maintainability	N/A
107	Be adequately flexible to keep up with ever changing technology and regulations	Non-Functional	Maintainability	N/A
108	Provide a high levels of performance, with acceptable response and processing times and application responsiveness at all times	Non-Functional	Performance	N/A
109	Be built to scale such that large increases users and usage can be accommodated in the future	Non-Functional	Performance	N/A
110	Provide response times of less than 5 seconds at all times	Non-Functional	Performance	N/A
111	Have seamless disaster recovery and backup processes	Non-Functional	Recovery	N/A
112	Adhere to all applicable legal, statutory, and regulatory requirements	Non-Functional	Regulatory & Policy	N/A
113	Have a low defect/failure rate	Non-Functional	Reliability	N/A
114	Provide reporting capabilities scalable to accommodate changes in system scale including changes in user population, transaction volume, throughput and geographical distribution	Non-Functional	Reporting	N/A
115	Provide the ability to build reports and save report templates These reports will have filtering capabilities and must be easy to build and modify by the administrative users	Non-Functional	Reporting	N/A
116	Provide business intelligence tools to allow for searching, reporting, and reviewing data for management purposes	Non-Functional	Reporting	N/A
117	Will allow users to quickly and easily develop and customize reports and queries to their own specific needs within a profile aligned to the analytic role of each user	Non-Functional	Reporting	N/A
118	Be implemented with a security infrastructure and tools for protection of programs and data from intentional unauthorized access attempts as well as security breaches due to accidental causes	Non-Functional	Security	N/A
119	Implement security controls in accordance with all Federal and State security policy and regulations and industry best practices	Non-Functional	Security	N/A
120	Allow for controlled access to participant records. Administrators and authorities will be able to view subsets of mDL related data based on user security privileges	Non-Functional	Security	N/A
121	Maintain a level of security that is commensurate with the risk and magnitude of the harm that could result from the loss, misuse, disclosure, or modification of information	Non-Functional	Security	N/A
122	Protect against possibly malicious user authentication attempts using an appropriate mechanism (e.g. locks the account/node until released by an administrator, locks the account/node for a configurable time period, or delays the next login prompt according to a configurable delay algorithm)	Non-Functional	Security	N/A
123	Provide the ability to identify certain information as confidential (e.g. PII) and only make that accessible by appropriately authorized users	Non-Functional	Security	N/A
124	When storing private information on any device intended to be portable/removable (e.g. smartphones, portable computers, portable storage devices), support use of a standards based encrypted format using 3DES, AES or their successors	Non-Functional	Security	N/A
125	Provide the capability to integrate with existing authentication and authorization mechanisms used by the Iowa DoT	Non-Functional	Security	N/A
126	Provide the capability to monitor events on the system, detect attacks, and provide identification of unauthorized use of the system	Non-Functional	Security	N/A

127	Implement advanced security through biometric functions taking advantage of functions built into leading mobile phone platforms	Non-Functional	Security	N/A
128	Prevent unauthenticated access to the mDL application	Non-Functional	Security	N/A
129	Bind biometric authentication methods to an instance of the mDL application to prevent impersonation of a user through the use of the mDL application	Non-Functional	Security	N/A
130	Communicate with other devices or networks only through encrypted connections	Non-Functional	Security	N/A
131	Provide user interfaces that are easy and efficient to use and well as conform to look and feel standards	Non-Functional	Usability	N/A
132	Support user-friendly navigation and interaction features that are easy to learn by a new end-user	Non-Functional	Usability	N/A

Comments